WHAT IS CLAIMED IS:

1. A recording/reproducing apparatus for recording in a recording medium the interleaved data with an error correcting code added thereto and reproducing the recorded data from said recording medium, the apparatus comprising an error correcting coding circuit for generating an error correcting code using an elliptic code on a finite field $GF(2^m)$ where m is a positive integer.

2. A recording/reproducing apparatus comprising:

an interface for converting an input signal to binary data;

an interleaver for segmenting the converted binary data into a plurality of data blocks;

a coding circuit for performing the error correcting coding operation for each of said data blocks using an elliptic code on a finite $GF(2^m)$ where m is a positive integer;

a signal processing circuit for converting the data block subjected to the error correcting coding operation into an analog signal for recording in a recording medium, and converting the analog signal read from said recording medium into binary data; and

a decoding circuit for detecting and correcting an error of the binary data converted by said signal processing circuit using said elliptic code.

3. A recording/reproducing circuit according to

Claim 1, wherein said coding circuit uses an elliptic code in which the length n of the data encoded for each interleave is not less than 2^m and the number t of correctable symbols holds the relation $m/2 < t \leq 2^{m/2}$, i.e. $m + 1 < 2t + 1 \leq 2^{(m+2)/2} + 1$.

4. A recording/reproducing circuit according to Claim 2, wherein said coding circuit uses an elliptic code in which the length n of the data encoded for each interleave is not less than 2^m and the number t of correctable symbols holds the relation $m/2 < t \leq 2^{m/2}$, i.e. $m + 1 < 2t + 1 \leq 2^{(m+2)/2} + 1$.

5. An error correcting coding method using a code having a check matrix wherein a point on an elliptic curve corresponds to the symbol location in such a manner as to continue in the ascending or descending lexicographic order of the direct product group G of the residue class ring of integers isomorphic with the elliptic curve as a group.

6. An information recording method comprising the steps of:

converting an input signal to binary data;

segmenting the converted binary data to data blocks;

subjecting each of said data blocks to the error correcting coding operation using an elliptic code on a finite field $GF(2^m)$ where m is a positive integer;

converting the data block subjected to the

error correcting coding operation to an analog signal; and

recording the data block converted to the analog signal in a recording medium.

7. An error correcting coding method wherein assuming that the reference position for counting symbols is the most significant order or the least significant order of the code and that in the case where a point on an elliptic curve corresponding to the jth symbol position as counted from the reference position is $P^{(j)} = (\alpha_j, \beta_j)$, the values $P^{(1)}$, $P^{(3)}$, $P^{(5)}, \ldots, P^{(2s+1)}$, where s is an integer, and 2s + 1 is n or n - 1, are arranged continuously in ascending or descending lexicographic order of the direct product group G of the residue class ring of integers isomorphic with the elliptic curve, and the relation holds that $\alpha_{2s+1} = \alpha_{2s+2}$ for $1 \leq 2s + 2 \leq n$.